ORNA™

Cybersecurity Advisory

Dear ORNA Customer,

We are sending you this advisory to provide situational awareness about a supply chain compromise around the tool Polyfill.js. This compromise not only affects the websites using it but also the end users visiting said websites.

Overview

In February of 2024, Polyfill.js library, a tool widely used to ensure compatibility of websites across different browsers, became the target of a supply chain attack. This attack was initiated when a Chinese company acquired the domain polyfill.io and its GitHub repository. Soon after, the attackers began injecting malicious code into websites using the library.

This malware targeted mobile users by redirecting them to fraudulent sites through a cleverly disguised fake Google Analytics domain. The malware was particularly insidious, as it only activated under specific conditions to avoid detection by website administrators and web analytics services.

The attack, nicknamed as Polykill, impacted over 100,000 websites, including notable users such as JSTOR, Intuit, and the World Economic Forum. Despite complaints from affected users, the new owners quickly removed these from the GitHub repository, making it challenging to address the issue promptly. The dynamic nature of the polyfill code, which adapts based on HTTP headers, presented multiple potential vectors for the attackers to exploit.

As a result of this breach, security experts and the original author of Polyfill have recommended against using the service, citing its redundancy with modern browsers' capabilities. Alternatives like those provided by Fastly and Cloudflare have been suggested for users who still require such functionality.

Recommendations

Recommendation #1: Block all requests to the domain

Orna recommends that organizations block any and all communication to the polyfill[.]io domain within their network and managed devices.

Recommendation #2: Remove Polyfill.js from your tech stack

Orna recommends that organizations using the polyfill tool remove it from their tech stack as soon as possible and seek alternative tools.

References

1. https://polykill.io/
2. https://sansec.io/research/polyfill-supply-chain-attack

If you have any additional questions, please reach out to your ORNA representative at sme@orna.app.

Sincerely,

ORNA Team